Parliamentary Assembly
Assemblée parlementaire
https://pace.coe.int

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Doc. 13481
08 April 2014

Improving user protection and security in cyberspace

Committee Opinion[1]
Committee on Legal Affairs and Human Rights
Rapporteur: Mr Arcadio DÍAZ TEJERA, Spain, Socialist Group

A. Conclusions of the committee

The Committee on Legal Affairs and Human Right commends the Committee on Culture, Science, Education and Media and its rapporteur, Mr Axel Fischer, on its report and draft resolution. It largely subscribes to the committee's conclusions and recommendations.

The committee recalls that it is currently undertaking further work on the protection of individuals against violations of their privacy rights in cyberspace and on the protection of whistle-blowers revealing abusive practices in cyberspace. It is in the process of preparing reports on "Mass surveillance" and on "Improving whistle-blower protection" (rapporteur for both subjects: Mr Pieter Omtzigt, Netherlands, EPP/CD).

The committee is of the opinion that the draft resolution would benefit from introducing the following amendments into its text.

B. Proposed amendments

Amendment A (to the draft resolution)

In the draft resolution, at the end of paragraph 3, add the following sentence:

> *"The objective must be an internationally agreed legal framework with appropriate enforcement mechanisms, including protection for whistle-blowers who disclose violations."*

Amendment B (to the draft resolution)

In the draft resolution, after paragraph 6.1, insert the following paragraph:

> *"collection, storage and processing of so-called meta-data (data that describes other data, for example information on senders, recipients, timing, key words, movements or contacts) shall be subjected, in principle, to the same rules as the collection, storage and processing of any other personal data;"*

Amendment C (to the draft resolution)

In the draft resolution, paragraph 6.3, after the words "while law-infringing users must be identifiable", add the words "and criminals must be identifiable by law enforcement bodies subject to the legal safeguards required under the European Convention on Human Rights (ETS No. 5);".

---

1. Reference to committee: Doc 12585, Reference 3772 of 27 May 2011. Reporting committee: Committee on Culture, Science, Education and Media. See Doc. 13451. Opinion approved by the committee on 7 April 2014.

C. Explanatory memorandum by Mr Díaz Tejera, rapporteur for opinion

1. **Amendment A** would strengthen the existing text, which is calling for a global initiative for improving user protection and security in cyberspace, to specify what the objective of such an initiative could be, namely to set up an internationally agreed legal framework with appropriate enforcement mechanisms. More details of this proposal will be included in the report under preparation in the Committee on Legal Affairs and Human Rights on "Mass Surveillance". But it can be said already now that a good tool to help enforce any legal restrictions on surveillance is solid protection for whistle-blowers who disclose violations of said legal framework. Due to the nature of the bodies carrying out surveillance (usually, secret services, whose supervision is very limited due to secrecy considerations) it will be very difficult to enforce any legal restrictions placed on surveillance in a credible way. The "sword of Damocles" of a whistle-blower safely disclosing any violations of the agreed rules may well be the most effective enforcement mechanism available.

2. The widespread perception that the collection, storage and processing of "metadata" is somehow not as problematic as that of the "content" of communications is false: the processing of metadata can provide an even more complete picture of the private life of a "target" than the processing of the content of communications, and should therefore be subjected to the same rules as the processing of other personal data (**Amendment B**).

3. With regard to **Amendment C**, the part-sentence to be replaced could be misinterpreted in order to justify a crackdown on the use of encryption, which is in turn the best way for ordinary Internet users to protect themselves from suspicion-free surveillance, and whose use the draft resolution is itself advocating in paragraph 6.2. In fact, all Internet users have the right to (try to) remain anonymous, whilst law-enforcement bodies have the right to (try to) identify perpetrators of illegal acts. The point is that they may invade the privacy of Internet users (in the same way as that of telephone or paper mail users) only under certain conditions defined by law (in particular, reasonable grounds for suspicion), as required under the European Convention on Human Rights (ETS No. 5)